UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,803	08/16/2001	Walter J. Schon	002.0212.01	3342

28875 7590 01/31/2006

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,803	SCHON ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *See Continuation Sheet* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *See Continuation Sheet* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/11/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Continuation of Disposition of Claims: Claims pending in the application are 1,3,5-7,10,12,14-16,19-20,22-24,26,28-30,32-33,35-37,39,42-43,45-46,48,51,53,56-58,60-61,63-65,67 and 70.

Continuation of Disposition of Claims: Claims rejected are 1,3,5-7,10,12,14-16,19-20,22-24,26-,28-30,32-33,35-37,39,42-43,45-46,48,51,53,56-58,60-61,63-65,67 and 70.

DETAILED ACTION

1. Claims 1 – 70 have been presented for examination. Claims 2, 4, 8 – 9, 11, 13, 17 – 18, 21, 25, 27, 31, 34, 38, 40, 41, 44, 47, 49 – 50, 52, 54 – 55, 59, 62, 66 and 68 – 69 have been canceled; claims 1, 10, 20, 26, 33, 39, 46, 51, 57, 60, 64 and 67 have been amended in an amendment filed 12/12/2005.

Response to Arguments

2. Applicant's amendment to the limitation of claim 1 has been fully considered and the 112 – 1st Paragraph rejection has been raised. See the following Office action.

3. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

4. As per claim 1, Applicant asserts: "prior arts fail to teach a verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such individual frame, and comparing the verification cryptographic hash and the original cryptographic hash". Examiner notes Applicant's arguments have been fully considered but are not persuasive because (a) Barton reference is relied upon providing the digital signature embedded into its own digital data block to enhance authentication capability (Barton: Column 4 Line 20 – 27) with a hash signature (Barton: Column 6 Line 37 – 44) as well as decrypting the encrypted original cryptographic hash using a decryption

cryptographic key (Barton: Column 7 Line 16 – 26), (b) Brothers reference is relied upon to disclose the authentication on a digital data block that can be a video frame (Brothers: Column 10 Line 48 – 49).

5. Furthermore, Applicant argues: "Tsuria fails to teach encryption cryptographic key utilized to encrypt each individual frame into encrypted video content". Examiner notes Brothers reference is relied upon providing "encryption cryptographic key utilized to encrypt each individual frame into encrypted video content" (Brothers: Column 10 Line 45 – 49) and Tsuria reference is relied upon to disclose storing the encryption cryptographic key is stored in a removable storage medium (Tsuria: Column 8 Line 54 – 56: for example, smart card).

6. As per claim 1, 10, 20,, 26, 33, 39, 46, 51, 57, 60, 64 and 67, Applicant further argues: "Tsuria does not teach a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames". Examiner notes the encrypted data will not be intelligent until the encrypted data is decrypted and accordingly, Tsuria teaches a validation module validating the decryption cryptographic key against user-provided credentials evidently prior to the decrypting function is performed (Tsuria: Column 8 Line 63 – 65) and Brothers reference is relied upon providing "the decrypting key and function are employed to decrypt the encrypted video frame" (Brothers: Column 10 Line 45 – 49).

7. As per claim 1, 10, 20,, 26, 33, 39, 46, 51, 57, 60, 64 and 67, Applicant further argues: "Tsuria does not teach a set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic

key and the decryption cryptographic key". Examiner notes (a) the broadest and reasonable claim interpretations are made such that a set of cryptographic instructions is interpreted as the executable instruction code that performs the cryptographic functions, (b) a smart card, as disclosed by Tsuria, generally contains a set of program instruction code that contains a seed generating algorithm for producing a seed which is used in signal scrambling at both ends of systems (Tsuria: Column 6 Line 63 – Column 7 Line 8).

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claim 1, 10, 20,, 26, 33, 39, 46, 51, 57, 60, 64 and 67 are rejected under 35 U.S.C. 112, first paragraph, as failing.to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The claim limitation of "a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium are capable of being utilized for encrypting the individual frames" is not enabled

by the specification. As understood by the examiner, this claim limitation is self-contradicting in the sense that the 1st limitation "a removable storage medium storing at least one of the encryption cryptographic key" is indeed contradicting with the 2nd limitation "a plurality of encryption cryptographic keys, each associated with a different removable storage medium" because the 2nd limitation discloses each cryptographic key of a plurality of encryption cryptographic keys is associated with a different removable storage medium while the 1st limitation recites a removable storage medium can store more than one of encryption cryptographic keys. Therefore, the invention of claim limitation is not clearly and concisely defined / specified in a manner which can be carried out by one skilled in the art.

Any other claims not addressed (are rejected) by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 3, 5 – 7, 10, 12, 14 – 16, 19 – 20, 22 – 24, 26, 28 – 30, 32 – 33, 35 – 37, 39. 42 – 43, 45 – 46, 48, 51, 53, 56 – 58, 60 – 61, 63 – 65, 67 and 70 are rejected

under 35 U.S.C. 103(a) as being unpatentable over Brothers (Patent Number: 5799083), in view of Barton (Patent Number: 5912972), and in view of Tsuria (Patent Number: 6178242).

As per claims 1, 10, 20, 26, 33, 39, 46, 51, 57, 60, 64 and 67, Brothers teaches a system for automatically protecting private video content using embedded cryptographic security, comprising:

a recorder frame buffer dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form (Brothers: see for example, Column 10 Line 45 – 52 and Column 9 Line 60 – 63);

an encryption module encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium (Brothers: see for example, Column 10 Line 45 – 52 and Column 9 Line 60 – 63: the digital tape is interpreted as transportable storage medium);

a decryption module retrieving encrypted frames from the transportable storage medium and decrypting each encrypted frame using a decryption cryptographic key that is verified prior to decryption (Brothers: see for example, Column 8 Line 23 – 27); and

a playback frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form (Brothers: see for example, Column 7 Line 44 – 47: the video signal must be

representing the raw video content in reconstructed form in order to be accessed by the viewfinder and external output stage as taught by Brothers).

However, Brothes does not disclose expressly a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium.

Barton teaches a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium (Barton, see for example, Column 4 Line 18 – 27, Column 4 Line 1 – 7 and Column 6 Line 37 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barton within the system of Brothers because (a) Brothers discloses the authentication of video frames using the encryption / decryption techniques (Barton: see for example, Column 2 Line 2 – 3), and (b) Barton further teaches providing a cost saving and efficient mechanism for the authentication of video frames by using a digital signature through a 16-bit checksum (i.e. hash value) of video frames (Barton: see for example, Column 4 Line 18 – 27, Column 4 Line 1 – 7 and Column 6 Line 37 – 42: using a digital signature through a 16-bit checksum (i.e. hash value)).

Brothers in view of Barton further teaches:

a verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such individual frame, and comparing the verification cryptographic hash and the original cryptographic hash (Barton: see for example, Column 4 Line 18 – 27, Column 4 Line 1 – 7, Column 6 Line 37 – 42, Column 4 Line 30 and Column 6 Line 37 – 44 & Brothers: Column 8 Line 23 – 27: Barton reference is relied upon providing the digital signature embedded into its own digital data block to enhance authentication capability (Barton: Column 4 Line 20 – 27) with a hash signature (Barton: Column 6 Line 37 – 44) as well as decrypting the encrypted original cryptographic hash using a decryption cryptographic key (Barton: Column 7 Line 16 – 26), (b) Brothers reference is relied upon to disclose the authentication on a digital data block that can be a video frame (Brothers: Column 10 Line 48 – 49).

Brothers in view of Barton further teaches a programmable memory to store at least one cryptographic key for use with the encryption and decryption algorithms (Brothers: Column 1 Line 59 – 61). However, Brothers in view of Barton does not disclose expressly a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

Tsuria teaches a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key (Tsuria: Column 8 Line 54 – 56: smart card is a removable security element).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barton within the system of Brothers because (a) Brothers discloses the authentication of video frames using the encryption / decryption techniques (Barton: see for example, Column 2 Line 2 – 3), and (b) Tsuria further teaches providing an enhanced security system to protect VCR recorded digital data streams (Tsuria: see for example, Column 1 Line 61 – 64).

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames (Tsuria: Column 8 Line 63 – 65 & Brothers: Column 10 Line 45 – 49: Examiner notes the encrypted data will not be intelligent until the encrypted data is decrypted and accordingly, Tsuria teaches a validation module validating the decryption cryptographic key against user-provided credentials evidently prior to the decrypting function is performed (Tsuria: Column 8 Line 63 – 65) and Brothers reference is relied upon providing "the decrypting key and function are employed to decrypt the encrypted video frame" (Brothers: Column 10 Line 45 – 49).

a set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key (Tsuria: Column 6 Line 63 – Column 7 Line 8: Examiner notes (a) the broadest and reasonable claim interpretations are made such that a set of cryptographic instructions is interpreted as the executable instruction code that performs the cryptographic functions, (b) a smart card, as disclosed by Tsuria, generally contains a set of program instruction code that contains a seed generating algorithm for producing

a seed which is used in signal scrambling at both ends of systems (Tsuria: Column 6 Line 63 – Column 7 Line 8).

As per claims 3, 12, 22, 28, 35, 58, 61 and 65, Brothers as modified further teaches providing the encryption and decryption algorithms in use of a public key system (Brothers, see for example, Column 2 Line 14 – 15). Official Notice is taken that the use of an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key for digital signature verification of is one of the well-known methods in the field.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key for digital signature verification.

As per claims 5, 14, 23, 29, 36 and 42, Brothers as modified further teaches an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key (Barton, see for example, Column 7 Line 19 – 26).

As per claim 6, 15, 48, and 53, see same rationale addressed above in rejecting claim 5.

As per claims 7, 16, 24, 30, 37 and 43, Brothers as modified further teaches a symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key (Brothers, see for example, Column 2 Line 11 – 12).

As per claim 19, 32, 45, 56, 63 and 70, Brothers as modified further teaches a computer-readable storage medium for performing the methods is provided as taught by Brothers in view of Barton (Brothers: see for example, Column 3 Line 34 – 62).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

Primary Examiner
AU 2131
1/25/06